UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,774	04/08/2004	Calum Murray	37202/136001;40098	1447

57956 7590 03/25/2009

OSHA - LIANG L.L.P. (INTUIT)
TWO HOUSTON CENTER
909 FANNIN STREET, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
03/25/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
lord@oshaliang.com
hathaway@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/821,774	MURRAY ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,7-10,13,15,16,19,21,22,25,27,28,31,33,34,36,37 and 39-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *,3,4,7-10,13,15,16,19,21,22,25,27,28,31,33,34,36,37 and 39-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 01/15/2009. Claims 1, 3, 4, 7-10, 13, 15, 16, 19, 21, 22, 25, 27, 28, 31, 33, 34, 36, 37, & 39-41 are pending and have been considered as follows.

Examiner Note

In light of the applicants' amendments and remarks, the examiner hereby withdraws his previous Claim Objections with respect to Claims 1, 7, 13, 19, 25, 31, 34, & 37 and withdraws his previous 35 U.S.C. 112 1st paragraph rejections with respect to Claims 1, 7, 19, 25, 31, 34, & 37.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 7, 13, 25, 31, 34, & 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allison ("pwdump - Windows NT password hash retrieval") in view of Guski et al. (US-5592553-A).

Claim 1:

Allison discloses a computer program product, comprising a computer readable medium storing computer executable instructions configured to control a processor comprising,

- "receiving a request from a user to obtain a file from a database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "wherein the user is associated with a user name" (i.e. "/* * Ensure we are running as Administrator before * we will run. */") [page 16];
- "obtaining, in response to the request, a file dump associated with the database" (i.e. "dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file") [page 1];
- "wherein the file dump comprises an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "decrypting the encrypted database password to obtain a database password" (i.e. "As this code decrypts the obfuscation step in the NT password database") [page 2];
- "wherein the database password comprises a hash value derived from the user name and password" (i.e. "allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "wherein the database password is associated with the user" (i.e. "account password") [page 2];

but Allison does not explicitly disclose,

- "obtaining a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest using one-time passwords in a system utilizing an access control mechanism for gaining access to resources, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain the file," although Guski et al. do suggest using one-time passwords in a system utilizing an access control mechanism for gaining access to resources, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];

- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain the file," in the invention as disclosed by Allison for the purposes of having ""one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 7:

Allison discloses a computer program product, comprising a computer readable medium storing computer executable instructions configured to control a processor comprising,

- "initiating a signon attempt to a database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "the signon attempt failing to connect" (i.e. "By default it will dump the password database of the local machine") [page 2];

- "wherein the failed signon attempt triggers an embedded mechanism within the database to dump an encrypted database password into a file dump" (i.e. "dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file") [page 1];
- "reading the file dump to obtain the encrypted database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "decrypting the encrypted database password to obtain a database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "wherein the database password comprises a hash value derived from a user name and password" (i.e. "allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "wherein the password is associated with the user name" (i.e. "account password") [page 2];

but Allison does not explicitly disclose,

- "obtaining a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;

- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest using one-time passwords in a system utilizing an access control mechanism for gaining access to resources, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," although Guski et al. do suggest using one-time passwords in a system utilizing an access control mechanism for gaining access to resources, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," in the invention as disclosed by Allison for the

purposes of having "'"one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 13:

Allison discloses a computer program product configured to control a processor to connect to a database comprising,

- "a computer readable medium" (i.e. "an NT machine that is held in the NT registry") [page 1];
- "an attempted signon module stored on the computer readable medium" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "the attempted signon module configured to communicate with the database to initiate a signon attempt to the database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "a read module stored on the computer readable medium configured to read a file dumped by the database" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "the file comprising an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "wherein the file is received in response to a failed sign on attempt" (i.e. "dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file") [page 1];

- "a decryption module stored on the computer readable medium configured to decrypt the encrypted database password to obtain a database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "wherein the database password comprises a hash value derived from a user name and password" (i.e. "allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "wherein the password is associated with the user name" (i.e. "account password") [page 2];

but Allison does not explicitly disclose,

- "a temporary signon module stored on the computer readable medium," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "the temporary signon module configured to communicate with the database to initiate a user session with the database to obtain a temporary user name based on the user name," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- "a pass connect string module stored on the computer readable medium," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

- "the pass connect string module configured to communicate with the database to pass a connect string to a database tool," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "the connect string comprising the database password," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "wherein the database, upon receipt of the connect string, allows the database tool to query the database," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a temporary signon module stored on the computer readable medium" and "the temporary signon module configured to communicate with the database to initiate a user session with the database to obtain a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights

associated with the temporary user name" and "a pass connect string module stored on the computer readable medium" and "the pass connect string module configured to communicate with the database to pass a connect string to a database tool" and "the connect string comprising the database password" and "wherein the database, upon receipt of the connect string, allows the database tool to query the database," in the invention as disclosed by Allison for the purposes of having '"one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 25:

Allison discloses a method of controlling a processor to connect to a database comprising,

- "initiating a signon attempt to a database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "the signon attempt failing to connect" (i.e. "By default it will dump the password database of the local machine") [page 2];
- "wherein the failed signon attempt triggers an embedded mechanism within the database to dump an encrypted database password into a file dump" (i.e. "dump the password database of the local machine") [page 2];
- "reading the file dump to obtain the encrypted database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "decrypting the encrypted database password to obtain a database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];

- "wherein the database password comprises a hash value derived from a user name and password" (i.e. "allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "wherein the password is associated with the user name" (i.e. "account password") [page 2];

but Allison does not explicitly disclose,

- "obtaining a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and,

optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];

- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," in the invention as disclosed by Allison for the purposes of having ""one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 31:

Allison discloses a computer program product, comprising a computer readable medium storing computer executable instructions configure to control a processor comprising,

- "hashing a user name and password to create a database password" (i.e. "it may be reversed, allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];

- "encrypting the database password to create an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "storing the encrypted database password in a database" (i.e. "the password databases") [page 2];
- "receiving a signon attempt for the database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "wherein the signon attempt fails" (i.e. "By default it will dump the password database of the local machine") [page 2];
- "creating a file comprising the encrypted password in response to the failed signon attempt" (i.e. "dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file") [page 1];
- "decrypting the encrypted database password to obtain the database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];

but Allison does not explicitly disclose,

- "obtaining a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;

- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," in the invention as disclosed by Allison for the purposes of having ""one-time" or "dynamic" passwords that are valid for only a brief time

interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 34:

Allison discloses a computer program product configured to control a processor to connect to a database comprising,

- "a computer readable medium" (i.e. "an NT machine that is held in the NT registry") [page 1];
- "a hash module stored on the computer readable medium configured to hash a user name and password to create a database password" (i.e. "it may be reversed, allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "an encryption module stored on the computer readable medium configured to encrypt the database password to create an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "a store module stored on the computer readable medium" (i.e. "an NT machine that is held in the NT registry") [page 1];
- "the store module configured to communicate with a database to store the encrypted database password in the database" (i.e. "the password databases") [page 2];
- "a send module stored on the computer readable medium" (i.e. "a 'AT' job on your NT server to periodically dump your NT password database into a new smbpasswd file and copy it over (securely somehow) to the Samba server") [page 1];

- "the send module configured to communicate with a launcher application to send the encrypted database password file to the launcher application" (i.e. "copy it over (securely somehow) to the Samba server") [page 1];
- "a launcher application stored on the computer readable medium" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "configured to: decrypt the encrypted database password to obtain a database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 2];

but, Allison does not explicitly disclose,

- "configured to: obtain a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "configured to: obtain a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," in the invention as disclosed by Allison for the purposes of having ""one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claim 37:

Allison discloses a method of controlling a processor to connect to a database and a launcher application comprising,

- "hashing a user name and password to create a database password" (i.e. "it may be reversed, allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "encrypting the database password to create an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "storing the encrypted database password in a database" (i.e. "the password databases") [page 2];
- "receiving a signon attempt for the database" (i.e. "/* *Open a connection to the remote machines registry. */") [pages 16-17];
- "wherein the signon attempt fails" (i.e. "By default it will dump the password database of the local machine") [page 2];
- "creating a file dump comprising the encrypted password in response to the failed signon attempt" (i.e. "dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file") [page 1];
- "decrypting, using the launcher application, the encrypted database password to obtain the database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];

but, Allison does not explicitly disclose,

- "obtaining, using the launcher application, a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining, using the launcher application, a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," in the invention as disclosed by Allison for the purposes of having ""one-time" or "dynamic" passwords that are valid for only a brief time interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

3. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Allison ("pwdump - Windows NT password hash retrieval") in view of Guski et al. (US-5592553-A) and in view of Prafullchandra (US-5734718).

Claim 19:

Allison discloses a method of controlling a processor to connect to a database comprising,

- "executing a launcher application" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "reading, using the launcher application, a file dump, stored in the database" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];
- "wherein the file dump comprises an encrypted database password" (i.e. "security = user encrypted passwords = yes") [page 2];
- "decrypting the encrypted database password to obtain a database password" (i.e. "NTCrack. Or you can get l0phtcrack") [page 1];

- "wherein the database password comprises a hash value derived from a user name and password" (i.e. "allowing a lanman and md4 hash to be written into the NT registry for a user account") [page 2];
- "wherein the password is associated with the user name" (i.e. "account password") [page 2];

but, Allison does not explicitly disclose,

- "obtaining a temporary user name based on the user name," although Guski et al. do suggest one-time passwords that are a function of secret or nonsecret information, as recited below;
- "wherein access rights associated with the user name are greater than access rights associated with the temporary, user name," although Guski et al. do suggest one-time passwords in a system utilizing an access control mechanism, as recited below;
- "logging onto the database using the temporary user name and the database password," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "accessing the database, based on the access rights associated with the temporary user name, to obtain a file," although Guski et al. do suggest usage of generated one-time passwords for authentication, as recited below;
- "wherein the launcher application is an embedded mechanism within the database," although Prafullchandra does suggest a database server side application which handles password recovery/changing, as recited below;

however, Guski et al. do disclose,

- "Systems of the type described in these references generate their one-time passwords as a function of secret information (such as a user password or an encryption key), time-dependent information such as a time-of-day (TOD) value or a time/date value, and, optionally, nonsecret information such as a user ID and application ID" [column 1 lines 64-67 & column 2 lines 1-2];
- "IBM Resource Access Control Facility (RACF)" [column 6 line 52];
- "If the transmitted password agrees with the comparison password, the user is authenticated and granted access to the system resource" [column 2 lines 7-9];

whereas, Prafullchandra does disclose,

- "The password update process runs on the server 18 and performs password updates according to the password aging information" [column 5 lines 44-46];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a temporary user name based on the user name" and "wherein access rights associated with the user name are greater than access rights associated with the temporary, user name" and "logging onto the database using the temporary user name and the database password" and "accessing the database, based on the access rights associated with the temporary user name, to obtain a file" and "wherein the launcher application is an embedded mechanism within the database," in the invention as disclosed by Allison for the purposes of having "'one-time" or "dynamic" passwords that are valid for only a brief time

interval (e.g., a minute or less), so that interception of such a password during one interval provides no useful information for gaining access to a system during a later interval" [column 1 lines 41-45].

Claims 3, 4, 9, 10, 15, 16, 27, 28, 33, 36, & 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allison ("pwdump - Windows NT password hash retrieval") in view of Guski et al. (US-5592553-A) and in further view of Kaufman et al. (US-5418854-A1).

Claims 3, 4, 9, 10, 15, 16, 27, & 28:

Allison and Guski et al. disclose a computer program product, comprising a computer readable medium storing computer executable instructions configured to control a processor, a computer program product configured to control a processor to connect to a database, and a method of controlling a processor to connect to a database, as in Claims 1, 7, 13, & 25, but their combination do not explicitly disclose,

- "wherein the database password is encrypted with a public key," although Kaufman et al. do suggest public key cryptography, as recited below;
- "wherein decrypting the encrypted database password is accomplished using a private key associated with the public key," although Kaufman et al. do suggest private key encryption, as recited below;

however, Kaufman et al. do disclose,

- "A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys" [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the database password is encrypted with a public key" and "wherein decrypting the encrypted database password is accomplished using a private key associated with the public key," in the invention as disclosed by Allison and Guski et al. since public key/private key pair cryptography is a common scheme of encryption for protecting information.

Claim 33:

Allison and Guski et al. disclose a computer program product, comprising a computer readable medium storing computer executable instructions for controlling a processor, as in Claim 31, but their combination do not explicitly disclose,

- "wherein the encrypted password is encrypted with a public key," although Kaufman et al. do suggest public key cryptography, as recited below;

however, Kaufman et al. do disclose,

- "A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys" [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the encrypted password is encrypted with a public key," in the invention as disclosed by Allison and Guski et al. since public key/private key pair cryptography is a common scheme of encryption for protecting information.

Claims 36 & 39:

Allison and Guski et al. disclose a computer program product for controlling a processor to connect to a database and a method for controlling a processor to connect to a database and a launcher application, as in Claims 34 & 37, but their combination do not explicitly disclose,

- "wherein the database password is encrypted with a public key," although Kaufman et al. do suggest public key cryptography, as recited below;
- "wherein the launcher application comprises a private key associated with the public key," although Kaufman et al. do suggest private key encryption, as recited below;
- "wherein the launcher application decrypts the encrypted database password using the private key," although Kaufman et al. do suggest public key cryptography and private key encryption, as recited below;

however, Kaufman et al. do disclose,

- "A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys" [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the database password is encrypted with a public key" and "wherein the launcher application comprises a private key associated with the public key" and "wherein the launcher application decrypts the encrypted database password using the private key," in the invention as disclosed by Allison and Guski et al. since public key/private key pair cryptography is a common scheme of encryption for protecting information.

4. Claims 21, 22, 40, & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allison ("pwdump - Windows NT password hash retrieval") in view of Guski et al. (US-5592553-A) in view of Prafullchandra (US-5734718) and in further view of Kaufman et al. (US-5418854-A1).

Claims 21 & 22:

Allison, Guski et al., and Prafullchandra disclose a method of controlling a processor to connect to a database, as in Claim 19, but their combination do not explicitly disclose,

- "wherein the database password is encrypted with a public key," although Kaufman et al. do suggest public key cryptography, as recited below;
- "wherein decrypting the encrypted database password is accomplished using a private key associated with the public key," although Kaufman et al. do suggest private key encryption, as recited below;

however, Kaufman et al. do disclose,

- "A well-known cryptographic technique used to perform remote authentication is public key cryptography. In this method of secure communication, each principal has a public encryption key and a private encryption key, and two principals can communicate knowing only each other's public keys" [column 2 lines 14-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the database password is encrypted with a public key" and "wherein decrypting the encrypted database password is accomplished using a private key associated with the public key," in the invention as disclosed by Allison, Guski et al., and

Prafullchandra since public key/private key pair cryptography is a common scheme of encryption for protecting information.

Claims 40 & 41:

Allison, Guski et al., Prafullchandra, and Kaufman et al. disclose a method of controlling a processor to connect to a database, as in Claim 19, but the combination of Allison, Guski et al., and Kaufman et al. do not explicitly disclose,

- "wherein decrypting the encrypted database password is performed by using a private key stored in the launcher application," although Prafullchandra does suggest public/private key cryptography is used where the private key is utilized for decryption of an encrypted database password, as recited below;
- "wherein decrypting the encrypted database password to obtain a database password is executed by the launcher application," although Prafullchandra does suggest a database server process that handles database password encryption/decryption, as recited below;
- "wherein logging onto the database using the temporary user name and the database password is initiated by the launcher application," although Prafullchandra does suggest a database server process that handles database password management, as recited below;

however, Prafullchandra does disclose,

- "It will be appreciated that only the client and the server can generate the common key since such generation requires either the client's secret key or the server's secret key which they only possess" [column 6 lines 4-7];
- "The password update process runs on the server 18 and performs password updates according to the password aging information" [column 5 lines 44-46];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein decrypting the encrypted database password is performed by using a private key stored in the launcher application" and "wherein decrypting the encrypted database password to obtain a database password is executed by the launcher application" and "wherein logging onto the database using the temporary user name and the database password is initiated by the launcher application," in the invention as disclosed by Allison, Guski et al., and Kaufman et al. since it is reasonable to expect that a database server would have an application/process/program which handles public key/private key pair cryptography for the purposes of automating the management of encrypted password information.

Response to Arguments

5. Applicant's arguments with respect to claims 19, 21, & 22 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicants' amendments.

6. Applicant's arguments filed 01/15/2009 have been fully considered but they are not persuasive.

- The applicants' argument, "Allison does not teach decrypting the encrypted database password to obtain a database password because it never obtains the fully decrypted password," has been carefully considered but is non-persuasive;
    - The examiner notes that in one particular embodiment Allison discloses "this code decrypts the obfuscation step in the NT password database" [page 2] which

suggests that upon dumping the encrypted database password is also decrypted to "plaintext equivalent" [page 2];

- Alternatively, as is written in the applicants' claims, it should be noted that if the decrypted database password is not plaintext but a hash value derived from the user name and password, it is reasonable to expect that the "decrypted database password" may be an intermediary form (once decrypted form) of the encrypted database password which is either encrypted multiple times or hashed and then encrypted;

- The applicants' argument, "…Guski does not teach wherein access rights associated with the user name are greater than access rights associated with the temporary user name…," has been carefully considered but is non-persuasive;
  - The examiner notes that Guski provides suggestion for varying levels of access with the incorporation of an access control system, where a one-time password has less access rights than a non-one-time password; therefore, it is reasonable to expect that with varying levels of access a one time password (i.e. a temporary password) would have less access even if that lesser right is merely access for a shorter duration of time.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
03/19/2009

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436